

CHAPTER 2



CH2. 轉動數位責任

2.1 創新管理.....	39
2.2 資訊安全.....	42
2.3 客戶權益保障	51

2.1 創新管理

2.1.1 創新投入與研發

橘子向來以滿足消費者生活需求為目的，透過各事業群互聯整合，打造全方位創新管理。研發策略上，橘子朝著「壯大集團 IP 生態圈，持續茁壯全方位娛樂生態」願景，執行自有 IP 開發與泛娛樂內容佈局，建構最貼近新世代態度與文化的社群平台，並持續投入行動遊戲及行動生活 App 之開發，及搶攻雲端與資安市場。2023 年研究發展支出達 6.53 億元，較前一年度提高 34.6%，台灣地區核准與公開之專利共 86 件。未來將持續引入 AI 新科技及技術，善用各事業群資源及數據優勢，全面深入生活運用，翻轉使用經驗，創新集團能量，發揮集團綜效，建構全生態娛樂網路企業，奠定永續成長動能。

2023 研究發展成果

✦ 「fun市集」打造正版授權IP的數位收藏品平台

✦ 「區塊鏈BaaS一站式整合服務」

✦ IP多元場景應用

✦ 《便利商店 口袋版》自製手遊，集團經典經營模擬IP，擴大虛實結合體驗

✦ 櫻桃小丸子手機遊戲上線，建立三消遊戲基礎框架供後續遊戲應用




✦ 研發AI美術、語音、文本、音樂等技術，並融入於開發過程中，提高產能及品質

✦ 完成霹靂核心玩法，展示核心戰鬥及相關美術優勢

✦ 提供創新AI智能客服，增加客服效率與精準服務

創新 IP 發展

台灣擁有豐沛的原創能量，卻因缺少資源而無法順利推展。橘子回應市場趨勢，於 2023 年底宣布將明年度將啟動三大計畫並設立目標，包括原創作品數量要成長超過 60%、平台點閱數破千萬，並朝跨域發展、招募新秀和深化人才培育三面向，未來也將輸出亞洲市場，進一步帶動集團生態系流量及業務，挹注橘子整體營運。

 跨域改編	<p>推出跨域企劃，為用戶創造再升級的娛樂體驗；旗下原創作品《三個不結婚的女人》也將與跨領域夥伴合作，除了有實體書與舞台劇改編外，將陸續推出不同衍生應用，為粉絲帶來更多驚喜。</p>
 新星計畫	<p>漫畫星、文學星推出「創作者平台」，提供創作者自行投稿的管道外，通過徵選還能成為站內「新星作家」或「官方簽約作家」。「新星作家」能參與官方舉辦進修課程並接受知名作家指導，也能提案爭取成為「官方簽約作家」</p>
 人才培育	<p>為正式簽約的作家提供穩定稿酬、助手補助、進修學習規畫並開展更多跨域創作可能性；與影視公司合作，針對漫畫小說與影視領域所需的編劇人才，合作培育課程以及與業界實作結合的培訓計畫；攜手大專院校漫畫系，提供學生創作以及未來出路的建議，助力學生與職涯接軌。</p>

創新多角化經營



遊戲橘子目標成為擁有高科技壁壘的國際網路集團，在多角化經營的策略下，以支持集團於網路科技產業的發展藍圖為導向，聚焦遊戲營運、技術研發和擴展 AI 科技應用範疇，期望透過內外部創新，提供更全球化的網路科技服務。

在內部創新方面，我們鼓勵員工進行內部創業，提供所需的創業環境、資金及各式資源，不僅能滿足員工追求自我實現需求、留住優秀人才，同時能促進組織活化，激盪出集團新成長曲線。

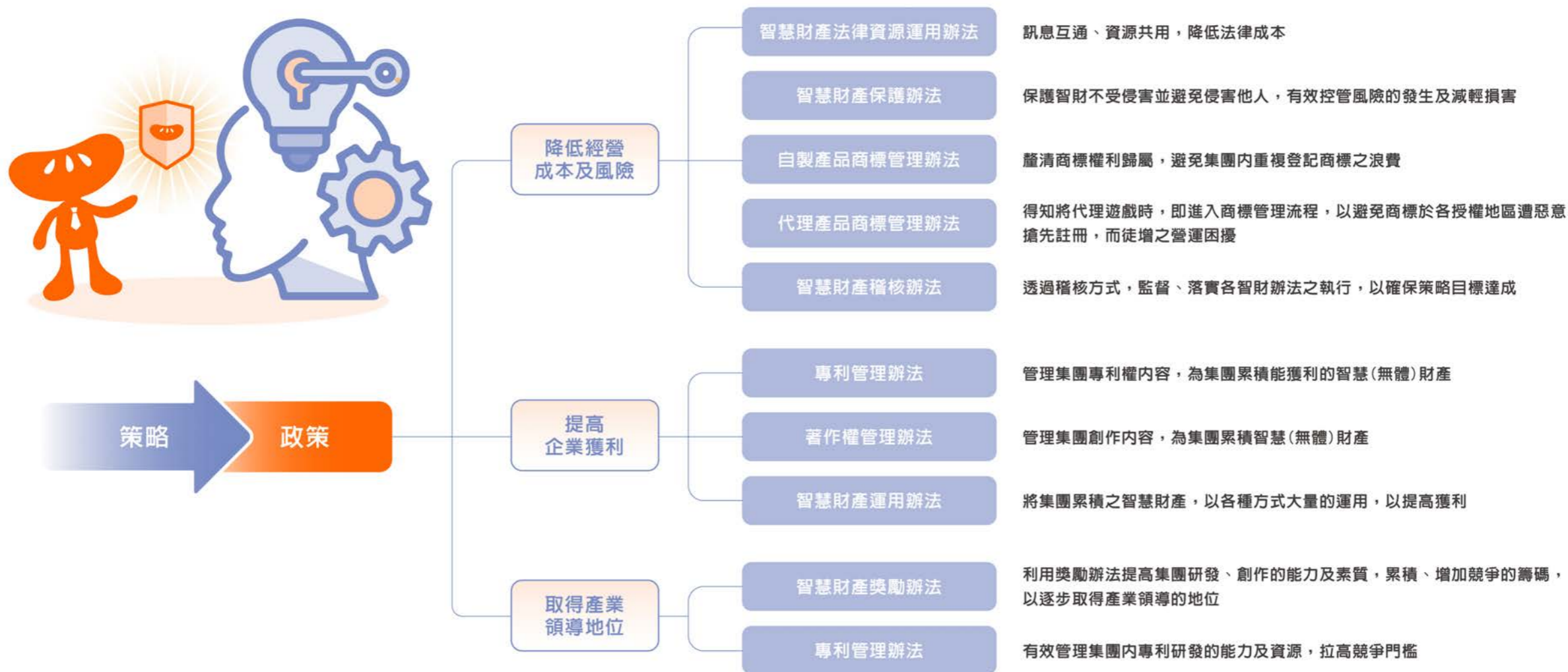
在外部創新方面，透過策略性投資新創企業，以獲得關鍵技術、加快產品開發速度，並取得具創新力的經營或技術團隊與人才，以提升集團競爭優勢及開發新事業發展機會，促進集團中長期營收及獲利成長動能。

專利策略目標

遊戲橘子集團致力於研發創新，根據營運目標投入研發資源，並擬定智慧財產權之管理計畫，藉以降低經營成本與風險，同時提高企業獲利、取得產業領導地位。本公司每年定期將智慧財產管理計畫提報至董事會，最近一次提報日期為 2023 年 11 月 06 日。

 技術領先	<p>持續投入相關服務的技術研發與專利布局，以維持產業的領先地位。</p> <ul style="list-style-type: none"> 完成專利探查與分析 <p>在連結公司營運目標的前提下，配合研發單位，針對下列領域進行檢索、分析：AI 詐騙偵測、AI 特徵學習、電子支付及 NFT 應用，以掌握業界技術發展動態與布局狀況，並進行對應的研發與突破，且將關鍵技術進行專利申請布局保護。</p>
 保護智權	<p>全面保護公司研發成果，嚴格要求專利、商標申請及著作權公證，落實集團智慧財產權政策。</p> <ul style="list-style-type: none"> 對於主要營運與計畫營運之地區進行萬筆商標查詢，且評估防堵與撤銷近似商標 計畫於 2024 年導入 TIPS 台灣智慧財產管理系統，促進內部智慧財產權管理制度升級與完善

為妥善運用及保護本公司之智慧財產，本公司訂有「智慧財產權基本政策」，以降低經營風險、提高企業獲利及取得產業領導地位，規劃本公司智慧財產權策略地圖。



2.2 資訊安全

2.2.1 資安管理

資訊安全政策

本公司訂有「資訊安全政策」由執行長核定，為本集團建立資訊安全、網路安全管理、程序及電腦系統軟硬體等相關資通管理之準則，以確保公司重要資訊之機密性、完整性及可用性。

資安治理組織架構

「集團資訊安全委員會」為本公司資通安全最高指導組織，由集團執行長擔任最高督導，同時督檢組織成員落實各項資訊安全管理作為，以表示對於資訊安全管理之充分支持。委員會組織構架如下，成員由各部門指派專員組成，包括且不限於首長、處級主管級別成員參與，集團總部於 2023 年設置「資安主管」，由資訊服務處處級管理單位綜理資通安全相關事宜，並委請專業資安技術團隊協助提供所需各項資安服務。年度召開兩次集團資安委員會議，由集團執行長主持，檢討現有安全管理制度執行情況、評估營運風險及相關因應方案及年度資安專案進度檢討。



「集團資訊安全委員會」基於集團營運目標、策略，遵照政府相關法令、法規要求，負責制定相應之資安政策，進行資安防護佈署、弱點漏洞補強、異常訊息掌握、緊急事件應變等，落實各項資安管理工作；秉承 PDCA(Plan- 規劃評估、Do- 設計建置、Check- 覆核稽查、Act- 檢討改善) 管理循環思維，以說寫做一致作為執行要點管理風險，以確保服務及營運持續。在風險評估、政策修訂、防護佈署、風險監控、安全補強的循環架構下，持續掌握新的資安趨勢，因應時空改變不同的資訊服務、營運環境、適法性及各項影響條件，滾動式檢討現行管理與防護作為，使資訊系統運營及網路服務均能做到適當的風險管控。

資訊安全管理策略與具體管理措施

本公司資安策略關注人員、制度及管理三大面向，遵循國家法令，通過風險導向的分析與管控，管理客戶及會員數字資產。

事前預防

- 定期檢討資訊安全相關管理規範

每年依照現行法令法規、產業脈動、關注方要求，進行資安政策及相關管理規範、程序編修作業，內容涵蓋資料保護、營運安全、資訊作業委外、密碼管理 ... 等共計 13 項規範。

- 資訊作業安全檢測

依專案性質進行風險評估，系統上線前依評估結果，進行行源碼掃描 / 弱點掃描 / 滲透測試等資安檢測，並確實完成系統弱點修補。

- 導入資安監控 (SOC) 及端點防護 (EDR) 機制

僱請國內第三方資安技術顧問團隊監控並掌握資安告警及情資，強化並加速偵防與回應。

- 資通安全作為有效性檢討

集團資訊安全委員會每年定期召開兩次會議，針對資安策略與機制進行滾動式的檢討與修正，同時檢討規範落地執行之成效並追蹤內部查核發現。

- 導入 ISO 27001 等國際資訊安全管理標準

強化資訊安全管理體系，訂定各項作業要求及應變處理計畫，提高整體資訊安全管控與應變能力。


- 集團各分子公司取得國際資安認證情形 (請參閱[資安認證一覽表](#))。

- 橘子支付自 2019 年起連年取得「行動應用 App 基本資安檢測」認證，並經第三方檢測機構通過。

- 社交工程演練及員工資安教育訓練

- 年度辦理電子郵件社交工程 1 次，另行針對誘騙成功之員工進行教育訓練。






- 年度實施資安訓練課程，並列為集團全員必修課程以全面性的提升同仁資安意識，完訓率 100%。

 事中執行與檢核	<ul style="list-style-type: none"> • 營運資訊作業自我評量 針對各項資安管理措設定評量機制，每季要求各營運分子公司進行資訊作業自我評量。 • 端點安全管理 設有端點防護機制，有效降低端點設備因不慎使用，形成資安缺口。 • 重要系統、資料庫及檔案皆具備份機制 每年針對核心服務系統設有系統復原計畫，定期（每年至少一次）執行災復演練，透過書面模擬及情境模擬演練，確認演練標的達成預設之目標、面臨緊急事件發生時能及時應對，確保服務不中斷。 • 年度資安內部查核作業 每年由集團總部擬定實施資安管理檢核計畫，對各營運分子公司進行訪談與抽樣各項資訊作業執行情況，並將查核結果提報集團資安委員會，查核發現則列管追蹤矯正情況，作為精進集團資安管理依據。
 事後應變與復原	<ul style="list-style-type: none"> • 建立資安應變及通報機制，確保資安事件可迅速及完善的處理與復原。 • 2023 年末發生重大的網路攻擊或事件，亦未曾涉入任何相關之法律案件或監管調查。

資安風險管理

公司資通安全風險管理是一個持續的過程，透過管理架構進行資通安全對營運風險分析及影響評估，建立適當防護機制、監控措施及應變作為，從而使公司營運做到以最小化損失和最大化收益。公司資通安全風險管理架構主要的目標是提供（1）營運所面對資通安全風險得到適當管理（2）鼓勵公司管理及運營團隊了解風險暴露的影響（3）實現更好的業務彈性和合規性（4）提供嚴格的決策和規劃流程。以下針對公司營運所可能遭遇之資安風險，提出說明及因應作為，確保公司營運服務和系統佈署了安全必要防護措施。



資安風險	影響及因應措施
 律法及標準合規性	<p>因應產業變動而生之律法要求，遊戲橘子因即時反應並滾動調整或增加相應管理制度以符合法遵要求。數位發展部於 2023 年 10 月 12 日頒布「數位經濟相關產業個人資料檔案安全維護管理辦法」，並依辦法施行之日起三個月內完成個人資料檔案安全維護計畫及業務終止後個人資料處理方法。本公司於 2024 年 1 月 12 日完成「個人資料保護政策」及「個人資料檔案安全維護計畫」，用以落地執行各環節資料處理與保護。</p> <p>本公司對標產業資訊安全標準合規性，透過第三方認證機構核實驗證實作，取得 ISO 27001 及 PCIDSS 認證並持續其有效性。</p>
 網路攻擊	<p>駭客使用技術手段或方法入侵、破壞或是竊取目標系統或網路，將直接衝擊企業營運，因此建置環境時應使用必要之防護措施，包括防火牆區隔、網段切割、安全通道存取設計規劃、使用加密通訊協定、設有入侵偵測及阻斷攻擊 ... 等機制；同時針對對外提供服務之網站定期或不定期進行相關之安全檢測（如：資安檢健、弱點掃描、滲透測試 ...）並修補弱點，及透過資安情資蒐集之弱點警示，進行系統強化或漏洞修補，以期減低因弱點而遭受攻擊之機率。</p>
 病毒威脅	<p>電腦病毒來源可能是瀏覽過的網站、電子郵件中含惡意程式的附件或連結、社交媒體網站的惡意連結或執行檔、可攜式儲存媒體、未經驗證文件、檔案、軟體或應用程式。因應種類廣泛的來源管道，公司設置多層次防禦機制及檢測，並全面導入端點防護系統，採中央管理方式進行監控及防護，以降低遭惡意程式感染及攻擊的風險。</p>
 營運中斷	<p>為確保企業營運持續，設有系統營運安全管理、備援及回復作業計畫之規劃及管理要求，而資安事件處理程序則是確保遭遇突發之緊急危難或異常事件時應及時反應與因應。維運依據「資安政策」、「集團營運事業資安管理要點」，年度針對營運核心服務進行資訊作業營運持續演練，驗證系統還原後能持續服務、確保機密資訊之安全性；同時演練含括事件通報處理，藉由完整的演練亦可讓相關同仁熟悉事件處理步驟，強化資安事件應變能力，減少營運衝擊，降低服務、資產及財務損失風險。</p>
 員工資安意識不足	<p>員工因職責需要，會直接接觸公司營運系統及資料，因此稍有不慎即可能因使用不明軟體或感染到惡意程式，而影響到公司内部系統資訊安全；因此公司除將自行編製之線上資安教育訓練列為必修課程，定期對全員工進行相關教育之外，日常蒐集資訊安全相關資訊及報導，不定期透過其它管道對員工宣導資安知識，用以降低不慎操作而造成資安風險的機會；同時也會透過社交工程演練驗證員工資安意識，提升員工對隱私權、個資法、數據保護實踐和網路安全行為等認知。鼓勵從事資訊技術職務的同仁，參加各式資訊安全、資訊作業管理 ... 之研討會，瞭解新興產業動態、資安趨勢及技術，用以提升自我技能，甚至藉此提升風險預判能力、及早防範。</p>

資安技術提升

橘子除持續在各分子公司導入 ISO 27001，為加強在端點防護與營運系統的安全性，導入了功能全面的 EDR 軟體，並整合 SOC 來確保防護與通報機制可以更加即時，並依據各子分公司的特性做對應的 EDR 防護政策導入，透過定期的資安技術會議，掌握集團的資安成效與交流最新的資安趨勢。

- EDR-端點偵測及回應：結合了即時的持續監控、端點資料蒐集，以及進階交叉關聯，來偵測並回應主機和端點連線的可疑活動，可讓資安團隊更快速的判斷及交叉比對分析並提供更明確的偵測事件。

在資安人才方面，果核數位作為集團的資安領導單位，針對職員之技術能量提升，制定資安人才培育辦法，依不同技術專業所適用之證照訂定不同金額津貼補助，藉以提升職員考取相關技術證照之積極度，使團隊技術能量有效提升。另外，2023 年集團辦理兩場次企業包班課程，展現本集團對於資安技術與人才培育重視。

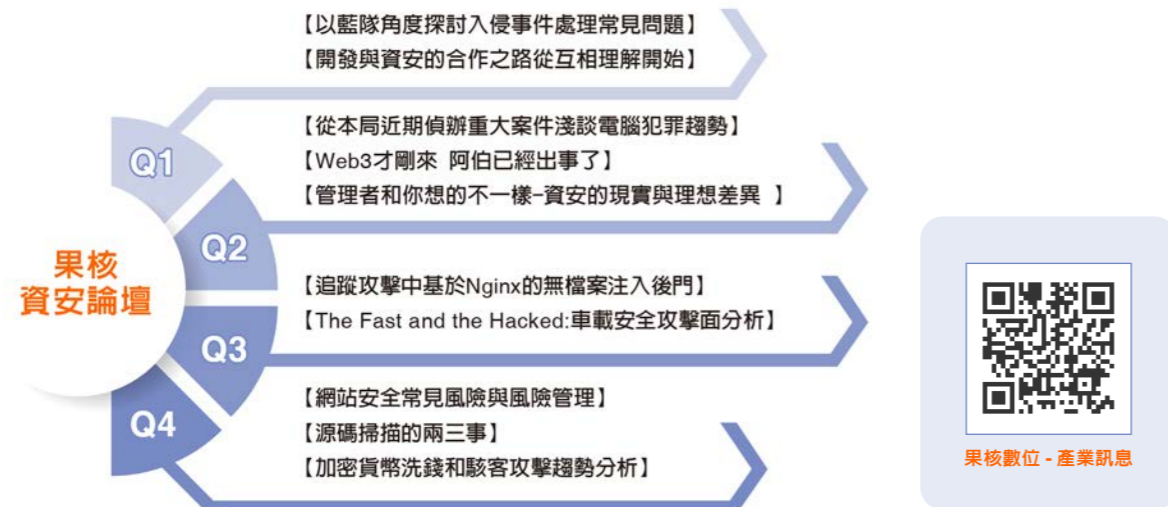
ISO/IEC 27001:2022 主導稽核員

本集團含分子公司，共計 16 名同仁上課，全數通過考試並取得證書。

零信任 & NIST 網路安全 全框架認知課程

邀請 BSI 講師授課，含營運長在內共 20 名學員完訓並取得上課證明。

因應 5G 時代來臨，駭客攻擊日新月異，橘子發揮產業專長，定期辦理果核資安論壇 (2023 年每季辦理一場次，共計 154 人次參與，平均活動滿意度達 99%)，亦於果核官網不定期分享資安相關文章，提高企業與個人對資訊安全防護之重視，並加強資安防禦層級，以避免因資訊外洩而造成損失及損害企業形象。



果核資安論壇

除內部主辦之論壇外，為引領業界驅動資安議題，果核也不定期與代理商及原廠合辦 Seminar 或 workshop，2023 年以「軟體開發安全」為主軸，攜手代理商邁達特及 OpenText，上半年舉辦【落實資安防護，杜絕漏洞風險】研討會；下半年舉辦【強化 DevOps 開發流程安全】說明會，不僅提供企業客戶軟體開發安全觀念，建議應將有限資源投入於關鍵刀口，更夠透過介紹 DevOps 全生命週期管理工具，帶領企業達到實踐敏捷資訊治理框架，以正確的思維主動尋找可能的風險，以釐清開發人員和資安人員雙方的認知。年末更自行舉辦 Source Code Analysis Workshop，透過實作的方式引導與會來賓了解程式開發的安全及重要性。

未來，果核數位將持續以實務經驗與溝通協助企業導入安排軟體安全測試，挖掘隱而未現的資安風險，強化軟體系統的安全性。

資安通報與處理程序

橘子訂有「資訊安全事件處理程序」，訂定集團各事業體資安事件通報及處理方式。集團全體同仁負舉發資安事件之責，一律立即主動告知所屬單位 IT 技術窗口，窗口須依其事件等級及分類進行釐清，填寫「資訊安全事件通報紀錄單」，責成資訊單位及事件相關單位做後續資安事件處理。資訊單位需於目標處理時間內排除及解決該事件，並於事件處理完畢後提供分析結果及建議修補作為，以預防事件重複發生。最後，上述的資安事件處理報告會彙整於資訊安全月報中，供資訊安全委員會議檢視留存。



供應商資安管理

橘子於 2023 年增設「資訊作業委外安全管理辦法」，為委外開發案做資訊安全審核，凡由第三方開發、建置、維護、處理與管理之活動，須依照其功能可能涉及之資安風險嚴重程度，具備相對應之資安檢測項目，包括重要數據隱私要求，確保每個供應商承諾應用足夠的技術和組織措施保護其處理的資訊。且資安檢測廠商資格需具備資安專業證照，並可提供原始碼檢測、弱點及滲透測試等檢測服務，使各分子公司之委外開發系統於導入或上線前具備標準安全性。此外，我們的法律團隊在處理和公司的數據交換（包括個資），確保所有供應商協議均應包括適當的陳述和關於保護的義務。

2.2.2 守護網路安全

集團對於所提供之商品或服務，除重視消費者之健康與安全，並對所提供的網路服務均向消費者詳細說明商品或服務之使用方法，維護交易之公平。對所提供的網路服務訂立預先擬定之契約條款，提供消費者充分與正確之資訊，及實施其他必要之消費者保護措施，以維護商品或服務之品質與安全，防止服務損害消費者之身心健康、財產或其他權益。對於商品或服務之標示、公平交易符合法令規定，提供完整消費資訊供運用，俾能採取正確合理之消費行為，以維護其安全與權益。

犯罪防治

網路資訊蓬勃發展，卻也伴隨著詐騙行為、盜取遊戲帳號等新型態社會問題。橘子秉持著服務客戶至上、玩家權益優先的態度，與大眾消費者站在同一陣線，凡收到相關的申訴案件，並有足夠的佐證資料，橘子團隊會主動出擊、與消費者並肩面對犯罪者，攜手消滅不良的投機者。自 2022 年開始我們與全民防詐騙網站（165）合作設置線上查詢平台機制，司法警察可藉由線上投單提出

查詢案件需求，提升作業效率。另外，為確保司法警察能及時了解數位遊戲相關的專有名詞，橘子成立獨立運作的「警偵小組」單位，派遣 24 小時輪班人力，隨時支援警察、檢調單位，提供資訊支援與疑問解答的服務，助力全民防詐騙不中斷。

GASH 是橘子的遊戲點數、虛擬商品，因近年電玩遊戲蓬勃發展，在市場已有大量、普遍性流通趨勢，卻也遭犯罪集團利用作為犯罪工具。

2023 年橘子與樂點 (Gash) 自 4 月起開始推出一系列風控管理措施，如「序號儲值延遲入點」、「點數防詐鎖卡平台」等，並設置「防詐工作小組」與數位發展部及警政署密切配合打詐，橘子不畏營運績效影響仍善盡產業自律與社會責任。截至年底已顯著減少近九成的詐騙案件發生，攔截逾 150 萬元，阻詐成效顯著。



橘子「全方位」打詐執行重點

風控管理：調整GASH錢包帳號與儲值風控管理

- 1 新創帳號身分認證：樂點與遊戲橘子皆針對新創帳號進行手機與電子郵件認證
- 2 強化帳戶驗證機制：樂點對GASH錢包用戶定期OTP驗證；遊戲橘子對平台遊戲帳號每日首儲進行OTP驗證
- 3 跳板IP儲值驗證：阻擋海外IP，不定時提供相關可疑IP供警方分析
- 4 序號儲值延遲入點：啟動GASH點數延遲入點機制，現況為延遲24小時入點，以爭取消費者辨識購買誘因及報案時間
- 5 異常帳號關閉儲值功能：針對新創、閒置、高風險帳號關閉序號儲值與轉點功能
- 6 點數防詐鎖卡平台：為保護消費者財產安全，於點數商品使用過程中疑似遭遇詐騙，可先行利用本平台進行商品鎖定避免被盜用



技術優化

與遊戲廠商協力打詐，並運用大數據演算法與後台資料分析，強化風控機制，技術端同步且持續分享予遊戲廠商

防詐宣導

集團媒體群與合作通路積極進行防詐騙宣導

攜手防詐

- 1 偕同通路合作廠商採取相關防詐措施與銷售監控，如與超商通路長期施行「主被動關懷提醒」機制、「單店每日銷售額度限制」、「單人單筆交易張數限制」與顧客「收執聯防詐提醒」等4項措施
- 2 聯合超商開發GASH去序號機制，推出「超商即時儲」，交易當下由系統直儲點數至遊戲帳號內的機制



橘子支付是橘子集團提供數位支付服務，主打交易、轉帳免用現金的特點，解決民衆攜帶現金可能面臨遺失或被搶奪等風險，卻難杜絕有心人士利用漏洞進行新型態電子詐騙的可能。近年橘子支付亦配合金管會加入電子支付阻詐行列，提出防堵措施，高度減少詐騙成功率，阻詐成效卓越。

橘子「電子支付」打詐執行重點

詐騙態樣	情境說明 (詐騙手法)	防堵措施	成效
冒開人頭戶後即有大額轉入，並迅速轉出	取得民衆身分證資料、手機門號及銀行帳戶後，向電子支付機構申請開立及註冊電子支付帳戶，進行跨行轉入金額，並快速跨行轉出	<ol style="list-style-type: none"> 1. 依照新修正之安全控管作業基準第 7 條，新增驗證會員開立存款帳戶或信用卡原留手機門號機制，以加強用戶身份確認 2. 高風險會員服務限權：潛在風險會員於首次單筆大額儲值時，再次發送確認簡訊並點選確認為本人後，始得開通大額儲值服務 3. 針對此態樣進行高風險會員服務限權：潛在風險會員於一定期間內，進行跨行轉帳限額 	<ol style="list-style-type: none"> 1. 防堵措施上線次月，警示帳戶當月數量降低至 0 件 2. 2023 年警示帳戶案件月平均數量較前一年度大幅減少 3. 財金轉帳、高風險通路受詐總額較前一年度分別減少 94% 及 46% 以上




產業法規推動

為了提升產業的競爭力，橘子協助政府制定維護公平正義且符合產業需求之法規，法務同仁亦擔任全國律師聯合會文創、運動及娛樂法委員會委員，透過各公協會長期向政府提出修法建議，並前往政府機關說明與分享。同時，每年度固定接受律師、司法官團體及學校法律相關科系學生參訪，了解在快速變動的數位娛樂產業中可能遇到的爭議事件，並交流對產業法規制度之看法。



數位內容責任

橘子集團之產品與服務多以數位娛樂多媒體內容為主，為提供玩家及消費者優質創新的服務體驗，所有數位內容之上架皆依循營運所在地法規之要求。除此之外，網路世界在民主的社會環境下，更加容易發聲，易伴隨不當內容的曝光風險，作為平台方，橘子主張應制定責任內容相關準則以傳達本公司在數位科技產業中的永續商業理念。

 廣告倫理	<p>2023 年本公司正式啟動「橘子集團廣告倫理政策」制定，為國內同業首家針對廣告主訂定廣告業務相關規範，並統合集團泛數位娛樂事業體之回饋，藉以提高本政策之適用性及作為產業示範。本政策內容除適法外，我們針對成人內容、管制商品、娛樂、健康等產品分類設定管制條件，並禁止一切暴力仇恨、騷擾、欺騙性文字以招攬或誤導消費者，如違反，橘子有權停刊該廣告。</p>
 責任內容	<p>本公司所發布的的遊戲及平台，於註冊頁面重點聲明使用者應遵守本公司營業規章、管理規則、網際網路國際使用慣例與禮節之相關規定，嚴禁任何違反公序良俗等行為，如具辱罵、誹謗、威脅、不雅等生成式內容，情節重大者本公司有權終止任何數位服務。</p>
 兒童保護	<p>本公司所產生之數位內容，為促進兒童青少年重視身心均衡發展，皆鼓勵年滿 12 歲以上的自然人使用，並應依照《兒童及少年福利與權益保障法》、《遊戲軟體分級管理辦法》規定，提供合適之數位內容及明確分級標章，採取避免兒少接觸之必要措施，並明確標示相對應之警語。所發布之遊戲及平台，皆於使用者條款提醒，我們尊重兒童及青少年的隱私權，對於未成年用戶或玩家，要求其法定監護人同意方可蒐集其個人隱私或敏感資訊。若家長 / 法定監護人有發現異狀，請立即連繫客服，橘子將採取適當措施保護兒童及青少年隱私。</p>



2.3 客戶權益保障

2.3.1 服務與溝通

橘子所有產品皆依據不同的業務範疇，遵照政府主管機關之法規及國際準則，制定相關服務機制及流程，以確保消費者或客戶在各項產品使用權益受到保障。我們將客服中心委任子公司蟻力，藉由 AI 技術提供全年無休 24 小時在線服務，同時因應不同產品需求，亦備有多元服務管道（電話專線、官網來信留言板、線上即時文字交談、智能 chatbot 客服等），讓客戶服務再升級。

專業客服體系

蟻力作為橘子集團的數據客服專家，掌握先進 AI 客服系統部署，人機協作，整合多元服務管道，精準提供客戶服務解決方案，同時提供顧客關係管理 (CRM) 整合服務，運用數據分析協助品牌維繫用戶忠誠度，有效管理品牌聲譽。全能的客服體系包含：

優質客服人員培育

- 通識課程：需全員參與及檢核完訓
 1. 基本服務認知及禮儀展現
 2. 產品專業知識及後台工具
 3. 權限使用規範、個資保護及資安風險
- 強化課程：視業務執行狀況安排
 1. 電話 / 親訪服務溝通談判技巧
 2. 情緒管理、建立正確服務心態
 3. 服務數據分析及報告撰寫

客服品質系統掌握

1. 智能客服渠道：風險字詞即時監測示警、負評案件普查並針對內容持續優化改善
2. 真人服務渠道：導入 AI 風控質檢針對風險案件即時監測示警 / 關懷、全渠道服務案件常態 3-5% 抽檢，針對缺失案件對外主動關懷更正資訊，對內則啟動個案輔導及強化資訊布達提醒

卓越解決方案服務

1. 擴大涵蓋 7*24hr 全時段即時問題諮詢回應
2. 針對障礙排查或需核資異動案型，引導自助服務功能操作，或留下需查核資料自動轉真人接手查核處理
3. 重要產品 / 活動資訊或案件處理進度即時通知、服務意見訪問調查



若為法人客戶，橘子依業務別定期與客戶安排相關會議，並與各單位高階主管做專案評估與檢討，確保產品及服務品質，即刻修正問題。因應本集團數位優勢，大部分事業體採用 AI 智能技術工具導入應用，不斷強化整體服務效能及互動品質，持續提升客戶服務體驗。重視客戶心聲，建立多元反饋機制，橘子支付更依主管機關規範，訂定且依循「客服營運中心品質政策」及其 13 份相關辦法，落實客服管理及客戶關係維運，保障客戶申訴權利。

2.3.2 隱私保護

橘子網路服務均設有防火牆、網路身份辨識、威脅監控分析機制並阻隔惡意網路行為、不定期針對網站系統弱點掃描並予以補強修正、不定期模擬駭客攻擊及資訊安全演練、依服務內容制定及實施備份作業等各項資訊安全防護措施，惟有經過授權的人員才能接觸到相關資料，詳細資訊請參閱 2.2 資訊安全。

橘子亦訂有「個人資料保護政策」，適用範圍涵蓋集團分子公司所有員工及其供應商，由集團「個資管理委員會」管理，針對集團內擁有個資之單位(包含全體員工、承包商及合同同業所管理之個資)，應規劃、執行與落實個資保護要求及委員會交辦事項，並向個資管理委員會報告個資保護推動進度。委員會以財務長為召集人，轄下分為緊急應變小組及個資保護工作小組，與法務處一同管理與防止外界不當侵入與維持個資檔案正確性及完整性。其中，個資保護小組納編「稽核小組」，由稽核室及法務處成員組成，規劃定期檢和安全維護計畫及相關規定之執行狀況，第一時間進行改善。

個資管理委員會之執行任務

1

個資保護政策之擬議。

2

個資管理制度之規劃及相關事宜討論、推展。

3

個人資料隱私風險之評估與管理審查。

4

集團所屬各級單位 以下簡稱各單位 專人與職員工之個資保護意識提升及教育訓練計劃之擬議。

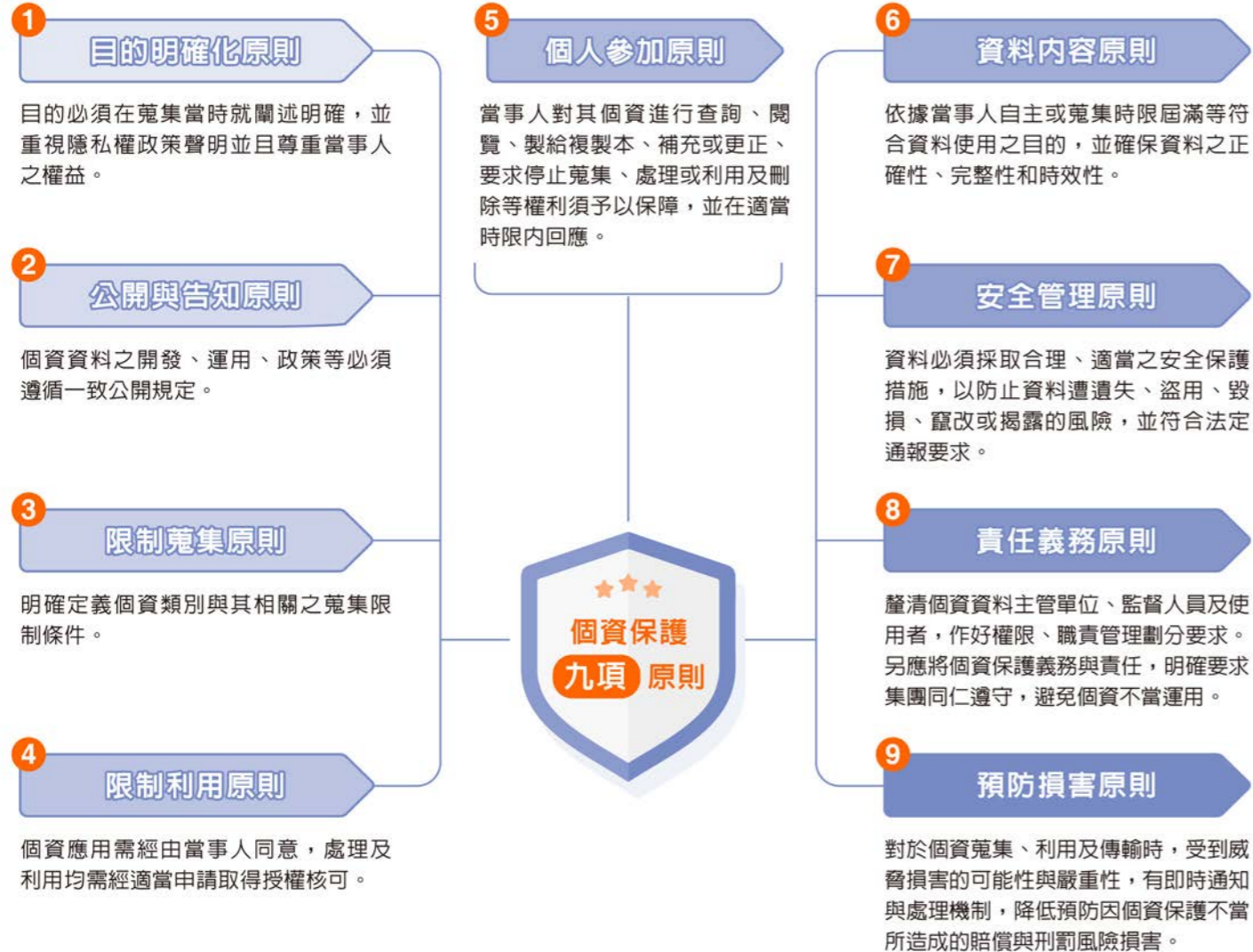
5

個資管理制度適法性與合宜性之檢視、審議及評估。

6

其它個資保護、管理之規劃及執行事項。

個資保護九項原則



橘子針對個資蒐集依循九項原則，任何個人資料的蒐集，皆主動告知客戶隱私權保護政策及使用者條款資訊、不蒐集不必要之個人資訊，並且告知用戶皆有權選擇是否被追蹤行為軌跡、做個人化行銷或二次目的使用。本年度個資被用於二次目的之使用者達 100%，主係橘子取得之個資將於後續線上線下活動中持續運用，直至該自然人主動申請停用或依平台隱私權條款進行調整（如因營運活動取得玩家資料，將依法規保存 5 年以上，公開資料皆會進行去識別化）。個資若經網路傳遞皆須加密機制，以確保資料在傳輸過程中不被第三方非法擷取。且依消費者或供應商簽訂服務約定，皆簽署保密條款，不會任意提供、出售、交換或出租的隱私與機敏資料給其他團體、個人、私人機構或其他用途。對於資安及個資保護業務，橘子以「零容忍」為原則，違者將依本公司「獎懲辦法」實施必要處置。2023 年並未發生侵犯客戶隱私事件，亦無與用戶隱私有關之法律裁罰。

2.3.3 客戶滿意度

一直以來橘子與消費者保持密切溝通與互動，積極守護消費者權益。橘子集團客戶服務以遊戲橘子之線上或手機遊戲為大宗，年服務量超過 75 萬件，有 92% 的案件可於首次回應獲得解決，服務品質檢核正確率達 99% 以上，同時以日、周、月、季、年為周期，透過系統檢視及統計分析案件問題，針對特殊、大量類型問題，提出因應及精進改善計畫，提交經營團隊作為評估，以降低重複客訴，並陸續上線多項自助化服務功能，透過技術賦能擴充智能客服涵蓋的服務項目，快速回應與解決客戶問題。2023 年總計公機關來函 871 件，其中 133 件須召開協調會，所有的客訴案件皆在 15 日內妥善處理完畢。2023 年並未發生無法解決、侵犯客戶隱私或健康等事件。

